PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-075601

(43)Date of publication of application : 26.03.1993

(51)Int.Cl. H04L 9/22

(21)Application number : 03-235007

(22)Date of filing : 13.09.1991

(71)Applicant : TOSHIBA CORP

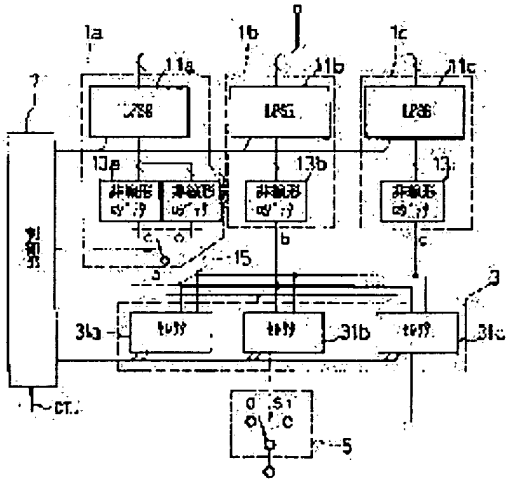
(72)Inventor : KITAGAWA KAZUO

(54) PSEUDO RANDOM NOISE GENERATOR

(57)Abstract:

PURPOSE: To provide a secure PN generating circuit from which the structure of a PN signal and of the PN generating circuit are not analyzed.

CONSTITUTION: The PN generating circuit is provided with noise generating means 1a, 1b, 1c, a replacement section 3 and a control section 7. The noise generating means 1 is constituted of a linear feedback shift register means 11 outputting plural pseudo random noise sequences with a control signal selecting plural sequences and a nonlinear logic 13 fetching plural output signals from the register means 11 and outputting one noise signal. The noise signal from each of the noise generating means 1a, 1b, 1c is given to the replacement section 3, in which various combinations are selected by using a switching signal Sk from the control section 7. The setting of the revision, switching and replacement of the noise generating means 1a, 1b, 1c and the replacement section 3 is revised at any time via the control section 7 and the analysis of the structure of a PN signal and a PN generating circuit is disable.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－75601

(43)公開日　平成５年(1993)３月26日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/22				
		7117－5K	Ｈ０４Ｌ　9/04	

審査請求　未請求　請求項の数３(全　7　頁)

(21)出願番号　特願平3－235007

(22)出願日　平成３年(1991)９月13日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　北川　和雄
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝映像メデイア技術研究所内

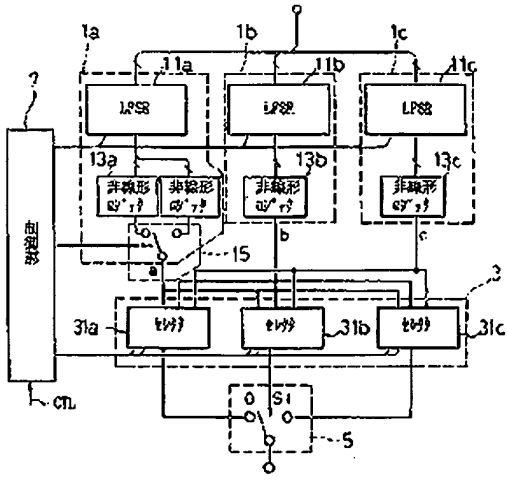
(74)代理人　弁理士　三好　秀和　(外４名)

(54)【発明の名称】　疑似ランダムノイズ発生装置

(57)【要約】

【目的】　ＰＮ信号及びＰＮ発生回路の構成を分析されない安全なＰＮ発生回路を提供すること。

【構成】　ＰＮ発生回路は、ノイズ発生手段１ａ、１ｂ、１ｃと、入替え部３と、制御部７とを備えている。ノイズ発生手段１は、複数のシーケンスを選択する制御信号により複数の疑似ランダムノイズシーケンスを出力する線形フィードバックシフトレジスタ手段１１と、前記レジスタ手段１１からの複数本の出力信号を取り込み、１本のノイズ信号を出力する非線形ロジック１３で構成されている。各ノイズ発生手段１ａ，１ｂ，１ｃからのノイズ信号は、入替え部３により制御部７からの切換信号Ｓｋにより各種の組合せに入れ換える。ノイズ発生手段１ａ，１ｂ，１ｃ．入替え部３の変更、切替え、入れ換えの設定を制御部７を介して随時変更可能とし、ＰＮ信号、ＰＮ発生回路の構成の分析不可能とした。



1

【特許請求の範囲】

【請求項1】　入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と、

入力される制御信号によって出力を変更し得る非線形ロジックで構成され前記線形フィードバックシフトレジスタ手段に接続される非線形ロジック手段と、

外部から入力される信号によって線形フィードバックシフトレジスタ手段と非線形ロジック手段に制御信号を与える制御手段とを有することを特徴とする疑似ランダムノイズ発生装置。

【請求項2】　入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と、

この線形フィードバックシフトレジスタ手段に接続され、入力される制御信号によって当該複数の線形フィードバックシフトレジスタ手段からの信号を入れ換える入換え手段と、

外部から入力される信号によって線形フィードバックシフトレジスタ手段と入換え手段に制御信号を与える制御手段とを有することを特徴とする疑似ランダムノイズ発生装置。

【請求項3】　入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と、

入力される制御信号によって出力を変更し得る非線形ロジックで構成され前記線形フィードバックシフトレジスタ手段に接続される非線形ロジック手段と、この非線形ロジック手段に接続され、入力される制御信号によって当該複数の非線形ロジック手段からの信号を入れ換える入換え手段と、

外部から入力される信号によって線形フィードバックシフトレジスタ手段と非線形ロジック手段及び入換え手段に制御信号を与える制御手段とを有することを特徴とする疑似ランダムノイズ発生装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、デジタルデータや音声のデータ列にスクランブルをかけるために使用される疑似ランダムノイズを発生する疑似ランダムノイズ発生装置に関する。

【0002】

【従来の技術】従来、疑似ランダムノイズ発生装置は、デジタルデータ列や音声のデータ列にスクランブルをかけるために使用される疑似ランダムノイズ（以下、単にPNと略称する）を発生するものとして提供されている。具体的には、例えば衛星放送の有料化の実現のために、このPN発生回路が使用されている。すなわち、衛星放送では音声をPCMデジタルデータで伝送しているが、これを有料化する場合には、一般的に音声のPCM

2

デジタルデータとPN系列とを排他的論理和（EXOR）回路で排他的論理和をとることによりスクランブルをかけ、盗聴を防止するようにしている。

【0003】図4は、上述したPN発生回路の簡単な構成例を示すブロック図である。図4に示すPN発生回路は、リニアフィードバックシフトレジスタ（LFSR；linear feedback shift register）で構成した例であり、シフトレジスタ401，403，405，407と、EXOR回路109とを備え、シフトレジスタ401をX，シフトレジスタ403をX^3，シフトレジスタ405をX^5，かつシフトレジスタ407をX^7とすると、その出力が（X^7+X+1）となるようにしてある。

【0004】そして、上記PN発生回路の出力は次のようになる。すなわち、例えば全"1"を読み込み、LFSRを動作させた場合、各レジスタ401，403，405，407の内容は、表1に示すようになる。

【0005】

【表1】

	X	X^3	X^5	X^7
1	1	1	1	1
2	1	0	1	1
3	1	0	0	1
4	1	0	0	0
5	0	1	0	0
6	0	0	1	0
7	0	0	0	1
8	1	1	0	0
9	0	1	1	0
10	0	0	1	1
11	1	1	0	1
12	1	0	1	0
13	0	1	0	1
14	1	1	1	0
15	0	1	1	1
16	1	1	1	1

【0006】上記表1の16番目のクロックは、元の全"1"の状態に戻って以下これをくり返すことになる。このとき、レジスタ407の出力（X^7）は"1110001001101011"の反復となる。このようなPN発生回路は、たとえレジスタの段数をn段に増加させて周期を長くしても、高々（2^n-1）にしかならず、極めて簡単にPN系列がサーチされてしまう虞が生じる。

【0007】この点を解消するために、図5に示すPN発生回路が提案されている。この図5に示すPN発生回

路は．ＬＦＳＲ５１１，５１３，５１５を有しており、各ＬＦＳＲ５１１，５１３，５１５には、３２〔ビット〕のスクランブル鍵である初期値ＩＫの１３〔ビット〕，１１〔ビット〕，８〔ビット〕として入力される。各ＬＦＳＲ５１１，５１３，５１５には、ロードタイミングＬＴ．シフトクロックＳＣｋが入力されている。各ＬＦＳＲ５１１，５１３，５１５には非線型ロジック（ＮＦ）５１７，５１９，５２１がそれぞれ接続されており、各ＮＦ５１７．５１９，５２１は各６〔ビット〕の入力を一本の出力にする。ＮＦ５１９は．切換信号を出力してスイッチ５２３を切り換える。ＮＦ５１７．１２１の出力は、スイッチ５２３で選択されてＥＸＯＲ回路５２５に入力される。ＥＸＯＲ回路５２５では．スイッチ５２３で選択された信号とＬＦＳＲ５１１からの出力との排他的論理和をとり．その結果ＰＮ信号として出力される。

【０００８】このように非線形化されて周期が長くしたＰＮ発生回路を使用し、さらにこれをカスタムＩＣ化することにより．実際上ＰＮ信号の構成がサーチされないようにしている（「電気通信技術審議会答申、諮問第１７号．昭和６３年１１月２８日」）。このようＰＮ発生回路によれば．出力系列を分析してＰＮ信号の構成をサーチする方法で使用してＰＮ信号の構成を分析しても分析が極めて困難であり、極めて安全性が高いといえる。しかしながら．カスタムＩＣチップの内部構成を顕微鏡で覗かれることまで考えると必ずしも安全とはいえなくなる。

【０００９】

【発明が解決しようとする課題】このように従来のＰＮ発生回路によれば、いくら複雑なＰＮ信号の構成にしても．そのＰＮ発生回路をＩＣ化した後のＩＣのチップを分析される方法に対しては安全といえないという欠点がある。

【００１０】そこで、本発明の目的は．この欠点を解消し．ＰＮ信号及びＰＮ発生回路そのものの構成を分析されない安全なＰＮ発生回路を提供することにある。

【００１１】

【課題を解決するための手段】上記目的を達成するために．本願第１の発明の疑似ランダムノイズ発生装置は、入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と、入力される制御信号によって出力を変更し得る非線形ロジックで構成され前記線形フィードバックシフトレジスタ手段に接続される非線形ロジック手段と、外部から入力される信号によって線形フィードバックシフトレジスタ手段と非線形ロジック手段に制御信号を与える制御手段とを有することを要旨とする。

【００１２】本願第２の発明の疑似ランダムノイズ発生装置は、入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と．この

線形フィードバックシフトレジスタ手段に接続され、入力される制御信号によって当該複数の線形フィードバックシフトレジスタ手段からの信号を入れ換える入換え手段と．外部から入力される信号によって線形フィードバックシフトレジスタ手段と入換え手段に制御信号を与える制御手段とを有することを要旨とする。

【００１３】本願第３の発明の疑似ランダムノイズ発生装置は、入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と．入力される制御信号によって出力を変更し得る非線形ロジックで構成され前記線形フィードバックシフトレジスタ手段に接続される非線形ロジック手段と．この非線形ロジック手段に接続され、入力される制御信号によって当該複数の非線形ロジック手段からの信号を入れ換える入換え手段と、外部から入力される信号によって線形フィードバックシフトレジスタ手段と非線形ロジック手段及び入換え手段に制御信号を与える制御手段とを有することを要旨とする。

【００１４】

【作用】上述した構成によれば、複数の線形フィードバックシフトレジスタ手段と非線形ロジック手段の構成を制御信号によって変更すると共に、さらにこれら出力信号を入れ換えの設定を随時変更することを可能にしたことにより、例えＩＣのチップを顕微鏡で分析されたとしてもなお、ＰＮ信号及びＰＮ発生回路の構成を分析不可能として安全性を高めたものである。

【００１５】

【実施例】以下．本発明について図示の実施例に基づいて説明する。

【００１６】図１は、本発明に係る疑似ランダムノイズ発生装置としてのＰＮ発生回路の実施例を示すブロック図である。図１に示すＰＮ発生回路は．３種類のノイズ発生手段１ａ．１ｂ，１ｃと、これら手段１ａ．１ｂ，１ｃからの出力信号を入れ換える入れ替える入替え部３と．入替え部３からの出力を切り換えるスイッチ５と、前記手段１ａ．１ｂ，１ｃの発生シーケンス及び入替え部３の切り換え制御する制御部７とを備えている。

【００１７】ノイズ発生手段１ａは．制御部７からの制御信号Ｓｃにより複数の疑似ランダムノイズシーケンスを出力する線形フィードバックシフトレジスタ手段１１ａと．前記レジスタ手段１１ａからの複数本の出力信号を取り込み、１本のノイズ信号を出力する二つの非線形ロジック１３ax．１３ayと．非線形ロジック１３ax，１３ayの出力の内の一つを制御部７からの切換信号Ｓｋで選択するスイッチ１５とから構成されている。ノイズ発生手段１ｂは．複数のシーケンスを選択する制御信号により複数の疑似ランダムノイズシーケンスを出力する線形フィードバックシフトレジスタ手段１１ｂと．前記線形フィードバックシフトレジスタ手段１１ｂからの複数本の出力信号を取り込み．１本のノイズ信号を出力する

5

非線形ロジック13bとから構成されている。ノイズ発生手段1cは、複数のシーケンスを選択する制御信号により複数の疑似ランダムノイズシーケンスを出力する線形フィードバックシフトレジスタ手段11cと、前記線形フィードバックシフトレジスタ手段11cからの複数本の出力信号を取り込み、1本のノイズ信号を出力する非線形ロジック13cとから構成されている。入替え部3は、前記各ノイズ発生手段1a，1b，1cからのノイズ信号を、制御部7からの入替信号Seにより各種の組合せに入れ換えるものであり、セレクタ31a，31b，31cから構成されている。各セレクタ31a，31b，31cは、各ノイズ発生手段1a，1b，1cからの出力信号を取り込み、入替信号Seにより一つ選択する。各セレクタ31a，31b，31cの出力はスイッチ5により一つ選択する。スイッチ5は、表2に示す信号が入力されている。

【0018】

【表2】

a	b	c
0	1	S
0	S	1
1	0	S
S	0	1
1	S	0
S	1	0

【0019】なお、上記制御部7は単なるラッチで実現できる。そして、制御部7から出力される制御信号Scは各レジスタ手段11a，11b，11cに各一本入力され合計3本となる。また、切換信号Skは1本、入替信号Seが6種の組合せとすると、この構成は$2^3 \times 2^3 \times 6 = 96$種をとりうることになる。この制御部7の制御信号Sc，切換信号Sk、入替信号Seの組合せは＊随時、送信局側からのコントロール信号CTLで変更することもできるし、このICを組み込んだ受信機に、何らかのキイ操作で構成したコントロール信号CTLで組合せを変えられることができるようにする。

6

【0020】図2は、線形フィードバックシフトレジスタ手段の構成例を示すブロック図である。図2において、線形フィードバックシフトレジスタ手段11a，11b，11cの各構成は基本的に同一であるため、符号a，b，cを取って説明する。線形フィードバックシフトレジスタ手段11は、シフトレジスタ111，113，115，117と、EXOR回路119，121と、アンド回路123，125とからなり、アンド回路123，125に入力される制御信号Scが"1"のときに$(X^4 + X^3 + 1)$の出力が、制御信号Scが"0"のときに$(X^4 + X + 1)$の出力が得られるようにしてある。一般にM段のレジスタ手段11a，11b，11cには、周期が$(2^n - 1)$になるいくつかの構成が知られており、3種以上のときは、制御信号Scを複数本とする必要がある。一般に、"1"と"0"の数を50%づつにし、入力変化に対し相関の少ない出力が出るようにされている。

【0021】図3は、非線形ロジックの構成例を示すブロック図である。非線形ロジック13ax，13ay，非線形ロジック13b、非線形ロジック13cは、一般にアンド回路、オア回路、EXOR回路の組合せで構成できるが、リードオンリメモリ（ROM）を使うのが最も簡単にできる。図3において、入力端子にスイッチ131を設けて7本のアドレス入力を可能にしている。スイッチ131を通して得た6本のアドレス入力をROM133に取り込み、一本の出力を得ている。ROM133は、表3に示すデータ例が記憶されている。ROM133は、表1に示す上位アドレスを2〔ビット〕、下位のアドレス4〔ビット〕に応じた値を出力できる。

【0022】

【表3】

上位＼下位	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	0	1	0	0	1	1	0	0	1	0	0	1	0	1	0
1	1	0	0	1	1	0	0	1	0	0	1	1	0	1	0	1
2	0	1	1	1	0	0	1	0	1	1	0	1	0	1	1	0
3	0	1	0	0	1	1	0	1	0	0	1	1	1	0	0	1

【0023】このように構成された実施例の作用を説明する。

【0024】制御部7は、各レジスタ手段11a，11b，11cに制御信号Scを与える。また、各レジスタ手段11a，11b，11cは、当該制御信号Scにより、例えば図2の構成から分かるように、制御信号Scが"1"なら$(X^4 + X^3 + 1)$の出力が、制御信号Scが"0"なら$(X^4 + X + 1)$が得られる。すなわ

ち．制御信号Ｓｃが"0"のときは．アンド回路１２５の出力がフィードバック信号１２７によらず"0"となり．ＥＸＯＲ回路１２１の片側の入力が"0"となる。すなわち、ＥＸＯＲ回路１２１は単なるバッファとなる。また、制御信号Ｓｃが"1"のときは、アンド回路１２３の出力．ＥＸＯＲ回路１１９の片側の入力が"0"となり．このＥＸＯＲ回路１１９が単なるバッファになる。このときは、別のＰＮシーケンスを発生することになる。このような出力信号を出力するレジスタ手段１１ａからは複数本の出力が非線形ロジック１３ax，１３avに、レジスタ手段１１ｂからは複数本の出力が非線形ロジック１３ｂに、レジスタ手段１１ｃからは複数本の出力が非線形ロジック１３ｃにそれぞれ入力される。非線形ロジック１３ax．１３av．非線形ロジック１３ｂ．非線形ロジック１３ｃは、それぞれ１本の出力を出す。非線形ロジック１３ax，１３avは、制御部７からの切換信号Ｓｋにより切り替わるスイッチ１５により一つが選択され．ノイズ信号ａとして出力する。非線形ロジック１３ｂからのノイズ信号ｂが．線形ロジック１３ｃからはノイズ信号ｃがそれぞれ出力される。各ノイズ信号ａ，ｂ，ｃは、入替え部３の三つのセレクタ３１ａ．３１ｂ，３１ｃにそれぞれ入力される。入替え部３のセレクタ３１ａ，３１ｂ．３１ｃには制御部７から入替信号Ｓｅが与えられており、これによりノイズ信号ａ．ｂ，ｃの内の一つが選択されて．表２に示すような６種の状態に入替えられる。各セレクタ３１ａ．３１ｂ．３１ｃの出力は、スイッチ５の"0"，"1"，"Ｓ"の入力に供給される。すなわち．三つのセレクタ３１ａ，３１ｂ．３１ｃは．三本のノイズ発生手段１ａ．１ｂ，１ｃからのノイズ信号ａ．ｂ，ｃをスイッチ５に入力して６種の組合せのどれかを選択する。

【００２５】このように本実施例では．制御信号Ｓｃ、切換信号Ｓｋ．入替信号Ｓｅの組合せは、随時送信局側からのコントロール信号ＣＴＬで変更することもできるし．このＩＣを組み込んだ受信機に何らかのキイ操作で構成したコントロール信号ＣＴＬで組合せを変えられることができるようにしていることから．ＩＣ化した内容を分析してもＰＮ発生回路の構成を簡単に変更することが可能であるため、ＰＮ発生回路の構成をサーチすることがほとんど不可能である。

＊【００２６】なお、上記実施例において、３種の方法で説明したが、２種の切替えとすることももちろん可能である。

【００２７】また、本実施例によれば．ＩＣをコピーされ海賊版が出回るっても簡単にＰＮ発生回路の構成を変更できるため．スクランブル放送への数億円の投資が全く無駄になってしまうことを防止できるという多大な効果を有する。

【００２８】

【発明の効果】以上説明したように本発明によれば、わずかな回路の追加により．容易にＰＮ発生回路そのものの構成を変更できるので．たとえＩＣを分析されても十分安全な、ＰＮ発生回路を提供することができる。

【図面の簡単な説明】

【図１】本発明の実施例を示すブロック図である。

【図２】本発明で使用するレジスタ手段の構成例を示すブロック図である。

【図３】本発明で使用する非線形ロジックの構成例を示すブロック図である。

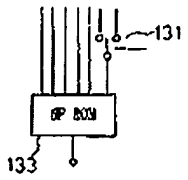
【図４】従来のＰＮ発生回路を示すブロック図である。

【図５】従来の他のＰＮ発生回路を示すブロック図である。

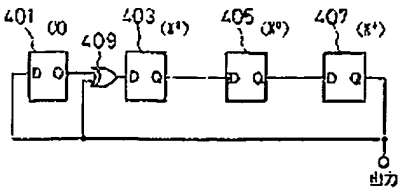
【符号の説明】

１ａ　ノイズ発生手段
１ｂ　ノイズ発生手段
１ｃ　ノイズ発生手段
３　入替え部
５　スイッチ
７　制御部
１１ａ　レジスタ手段
１１ｂ　レジスタ手段
１１ｃ　レジスタ手段
１３ax　非線形ロジック
１３av　非線形ロジック
１３ｂ　非線形ロジック
１３ｃ　非線形ロジック
３１ａ　セレクタ
３１ｂ　セレクタ
３１ｃ　セレクタ

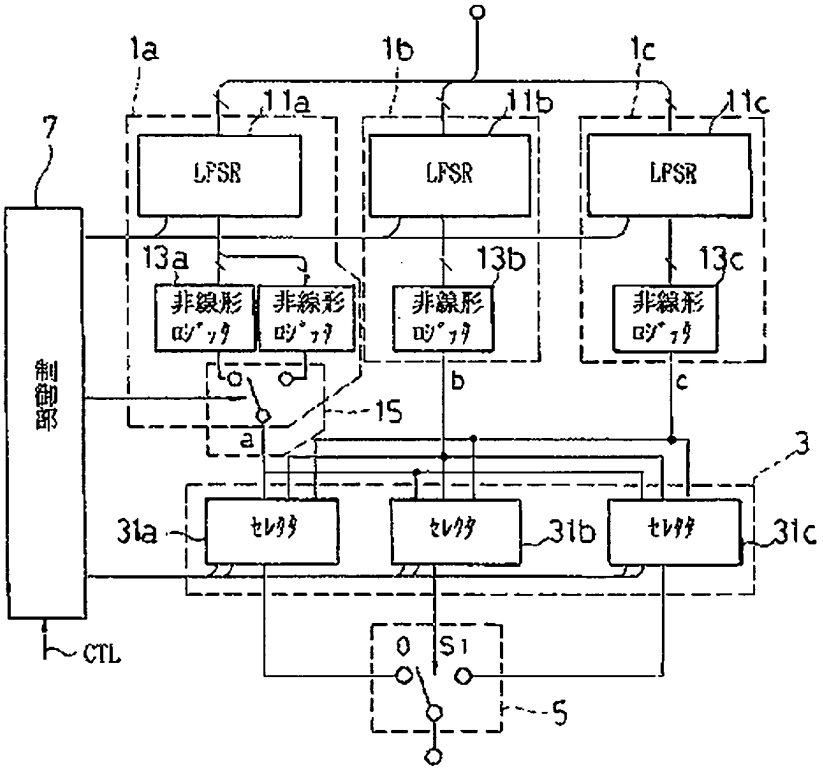
【図３】



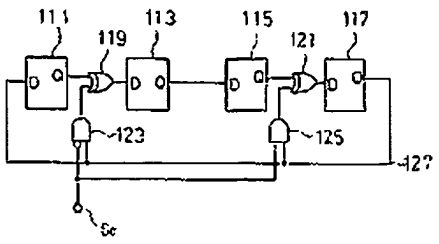
【図４】



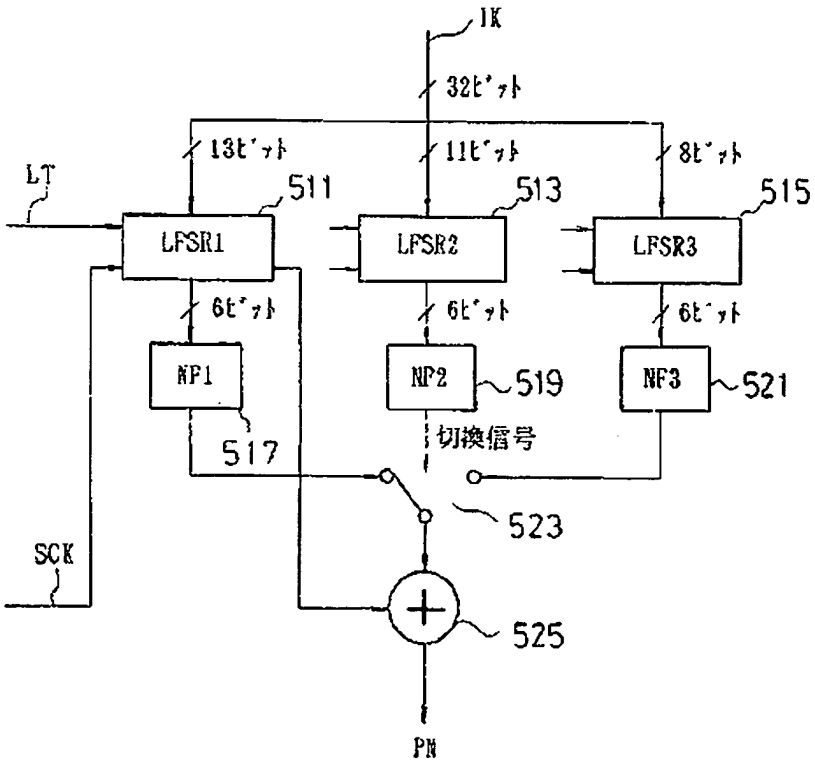
【図1】


1a
1b
1c
11a
11b
11c
7
LFSR
LFSR
LFSR
13a
13b
13c
非線形
ロジック
非線形
ロジック
非線形
ロジック
非線形
ロジック
制御部
b
c
15
a
3
31a
セレクタ
セレクタ
31b
セレクタ
31c
CTL
0
S1
5

【図2】


111
119
113
115
121
117
123
125
127
Sc

【図5】


IK
32ビット
13ビット
11ビット
8ビット
LT
511
513
515
LFSR1
LFSR2
LFSR3
6ビット
6ビット
6ビット
NF1
NF2
519
NF3
521
517
切換信号
523
SCK
525
PN